

ANDROID PRIVACY SETTINGS (ANDROID 10.0)



Best Practices

- Smartphones and tablets are not impenetrable. Secure your smartphone with a password or biometrics, and utilize apps such as **Find My Device** or **Prey Anti Theft** to locate lost or stolen devices.
- All smartphones and tablets have cameras and microphones that can be remotely activated. Consider your device when you are in certain places or conversations.
- Bluetooth and wireless capable devices are convenient but easily exploitable by hackers. Use a VPN if possible, and always avoid public wireless networks.
- Prior to downloading apps on your device, read the developer's permissions. Many apps request permission to access your camera, microphone, text messages, and phone contacts.
- Keep location services turned off until they are actually needed. Otherwise, your daily movements are likely being tracked. Don't worry, location services are always available to 911 and first responders, even when turned off.
- If you have a google account, you can use your google credentials to login at maps.google.com/locationhistory to see your device location history for the last year or more.

***NOTE:** Due to varying Android manufacturers, the instructions in this Smart Card may vary slightly depending on the device being used.*

The most important thing you can do to keep your information secure is to keep your device up to date. In order to make sure your Android is up to date with the latest Android Version, first go to "Settings" then "System," scroll to the bottom and select "Advanced." From there you will see the "System Update" tab, select the tab. (On some versions, you may go to "Settings", then "Software update" toward the bottom of the "Settings" list).

Physical Security

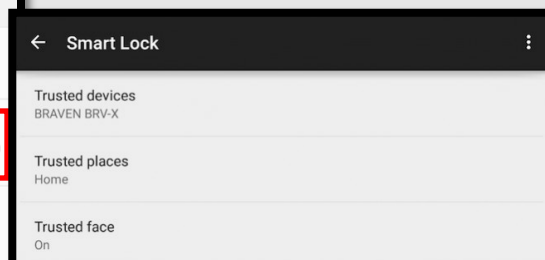
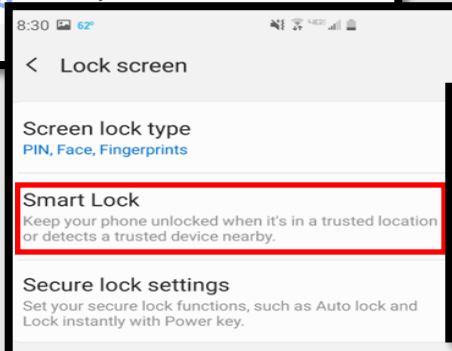
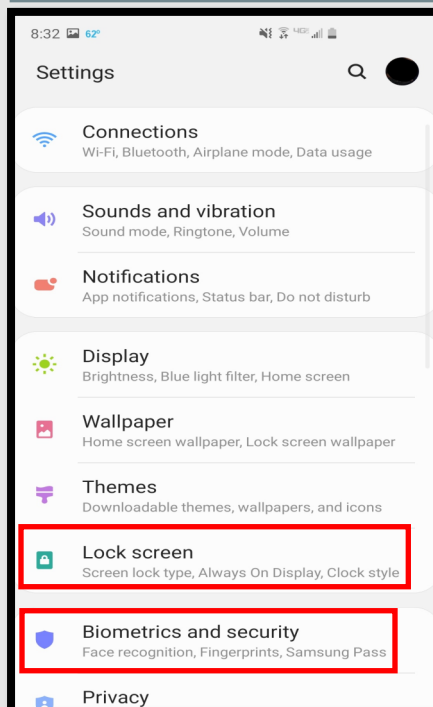
The first line of defense in preventing unauthorized access to your device is to protect it with a "Passcode". In addition, Android 9.0 offers several enhanced security features, including "Fingerprints", "Facial Recognition", "Encryption", and "App-level Permissions".

Under "Settings", first select "Biometrics and security". Here, you can set up your "Face recognition" and "Fingerprints" profiles. You will then go back to "Settings" and select "Lock Screen" in order to set your screen-lock preferences. Tap the "Settings" icon and then tap "Lock Screen." The options are Swipe, Pattern, PIN, Password, Face, Fingerprints. The most secure way to protect your phone is to use the **biometric** options, such as "Face Recognition" and "Fingerprints". A "Password" is the strongest backup solution.

Also under "Lock Screen", you will see the feature "Smart Lock", which allows you to set "Trusted Places" inside of which your device will unlock itself and remain unlocked. This feature can be set to recognize your face and "Trusted Devices" as well, all of which trigger your device to "Unlock" and remain unlocked. This feature is meant for your convenience, but presents obvious vulnerabilities. We recommend you do not enable any "Trusted Features".

Under the "Biometrics & Security" section, you may be able to select the option to "Encrypt Phone", which allows you to initiate the encryption of all data on your device. According to the instructions, this could take up to an hour and requires your device to be plugged into its charger. This process must not be interrupted, so be

sure to start it when you are sure you will not need to use your device for that amount of time. You will only need to perform this once. Locking your device encrypts the data on your phone. Unlocking your encrypted device decrypts your data.

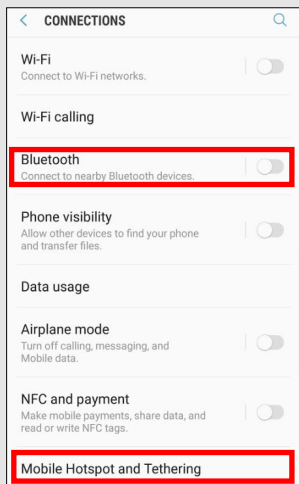


ANDROID PRIVACY SETTINGS (ANDROID 10.0)

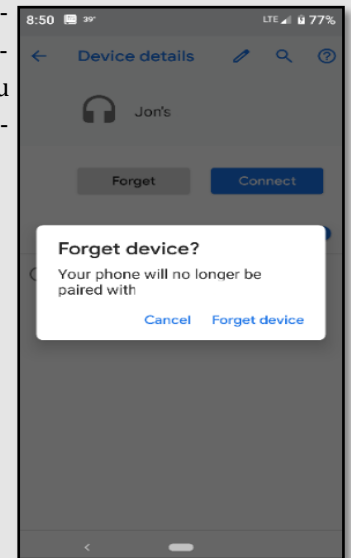
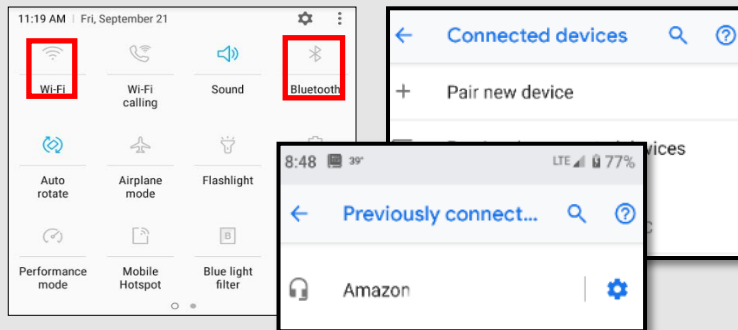


Mobile Hotspot and Bluetooth

Mobile hotspots are areas away from your home where your internet company provides you with Wi-Fi. Alternatively, hotspot devices can be purchased and used for connecting to the internet remotely, but without connecting to public Wi-Fi, which we always discourage. Most Android Smartphones have a “hotspot” feature that allows you to connect to your internet (for instance on your laptop) remotely. By turning on this feature, your phone uses its cellular data to create a “Wi-Fi hotspot”. Then, you can connect to this hotspot with a computer or another device that does not have cellular data. You can turn this option on and off under “Settings” > “Wireless & Networks” or “Connections” > “Mobile Hotspot and Tethering”. **Bluetooth** is a wireless technology for exchanging data over short distances from fixed and mobile devices. When Bluetooth is enabled on your device, hackers could gain entry to your device and obtain contacts, messages, calendars, photos, and notes, or install malware without you even knowing. To disable Bluetooth go to “Settings” > “Wireless & Networks” or “Connections”.



Wireless Networks



Note: We always recommend avoiding public Wi-Fi networks because they are unsecured. If you must use one, avoid logging into accounts that require passwords and use a VPN client to encrypt on-line transactions.

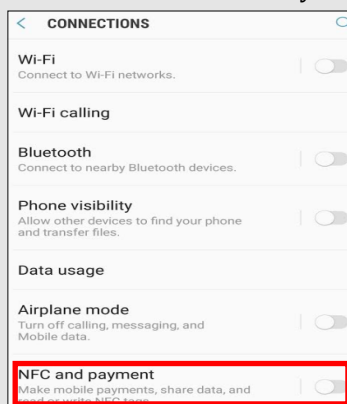
Note: In order to delete Bluetooth sessions you no longer need, go to “Bluetooth”, select “Previously Connected Devices” then select the “Settings” icon, select “Forget.”

Note: From the “Quick Settings” drag-down tray, tap and hold “Wi-Fi” to see available networks. Tap the “Wi-Fi” icon to turn Wi-Fi “off” when not in use.

Near Field Communication (NFC)

NFC is a set of short-range wireless technologies, typically requiring a distance of 4cm or less to initiate a connection. The technology allows you to “bump” your smartphone with other NFC devices to exchange information or pay for items using a Pay app. Although extremely close range, a malicious user can tamper with the data being transmitted between two NFC devices if they are within range. NFC risks include: data tampering, data interception, and mobile malware.

Turn off NFC when not in use by tapping “Settings” > “Wireless & Networks” or “Connections”. Then tap the toggle switch for “NFC and payment” so that it is in the “off” position.

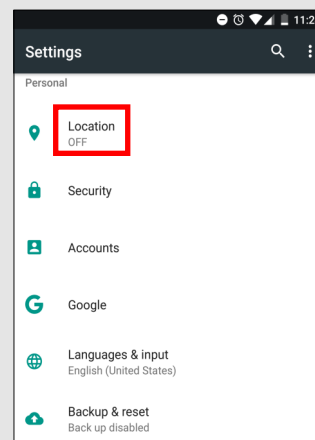


Location Services

Whenever you take a photo, data on your location is saved inside of the photo’s EXIF data. When you send that photo to someone or post it online, data on where you took the photo may be available to those who know how to view it. If you post a picture that you took from your home, anyone that can view it may be able to figure out where you live and more.

To disable your location from being shared, select “Settings” and scroll down to “Biometrics and security.” Disable your location services by switching the toggle to “off”.

* Newer device “Location” function is separately under “Settings”, just below “Biometrics and security”.



ANDROID PRIVACY SETTINGS (ANDROID 10.0)



Lost/Stolen Phone

Over 100 cell phones are lost or stolen in the U.S. every minute, which shows how necessary it is to keep your device secure and locked with biometrics or a passcode. All Android phones work by synching a phone to a google account, so if you lose your device, you can go to **android.com/find** in order to locate it. This is the native “Find My Device” tool for Android, and is automatically enabled on your Android Smartphone. Alternatively, you can download the “Find My Device” app from Google Play Store.



- ◆ Locate Android devices associated with your Google account.
- ◆ Reset your device's screen lock PIN.
- ◆ Erase all data on the phone.

Note: If you turn off “Location Services” in the “Location Setting” menu, you cannot use “Location Services” for apps that locate lost or stolen devices. You can still wipe your phone if the “Location Services” are “off”. If you wish to use some “Location Services”, be sure to go into each app and set the “Location Settings” as desired rather than turn off the main “Location Services” setting.

What should you do if your device is lost or stolen? Google can help you locate it. Let's enable the settings on your device so that in case you need to, you can locate your lost phone.

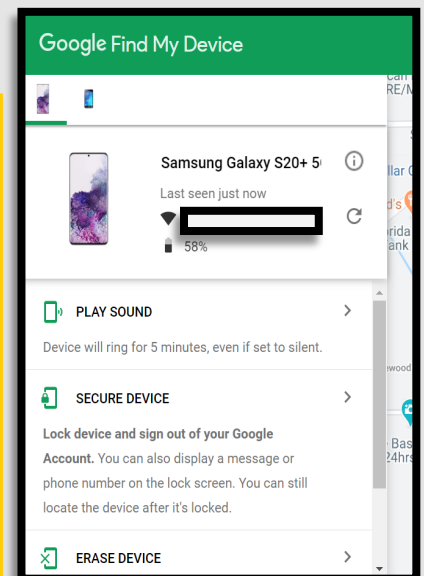
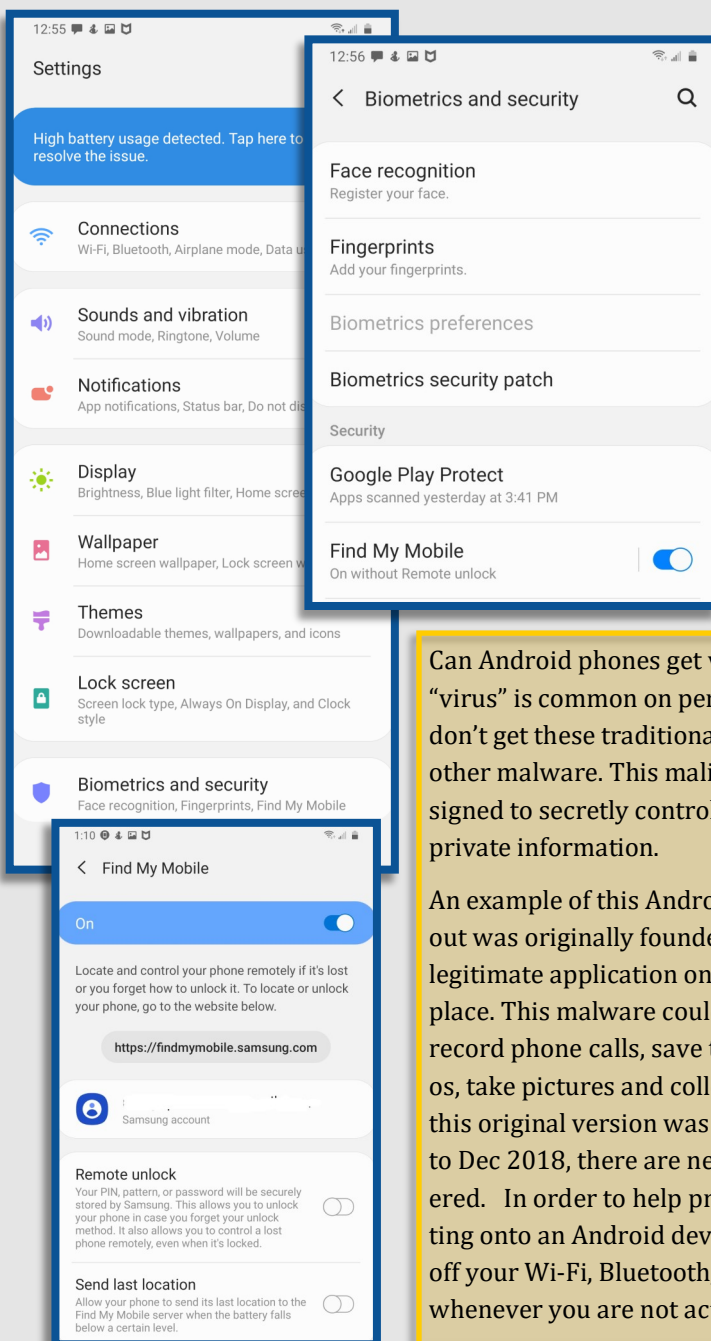
Go into “Settings” > “Biometrics and security” > “Find My Mobile”. Ensure the Toggle is set to “On”

If your device is lost or stolen, you can then go to “Google Find My Device” page and see where your phone was located last. You can make the (**android.com/find**) device ring at full volume to help you find it or remotely lock or erase all data on it.

In order to test this feature, let's go to **android.com/find** and see if it works.

Can Android phones get viruses? The traditional “virus” is common on personal computers, Androids don't get these traditional viruses, but they do get other malware. This malicious software can be designed to secretly control the device or even steal private information.

An example of this Android malware is Triout. Triout was originally founded in 2018, bundled with a legitimate application on the Google Play marketplace. This malware could hide on your Android and record phone calls, save text messages, record videos, take pictures and collect your location. Although this original version was only active from May 2018 to Dec 2018, there are new variations being discovered. In order to help prevent malware from getting onto an Android device it is important to turn off your Wi-Fi, Bluetooth, and sharing capabilities whenever you are not actively using them.



ANDROID PRIVACY SETTINGS (ANDROID 10.0)



Lost or Stolen Android Device

Ad Tracking

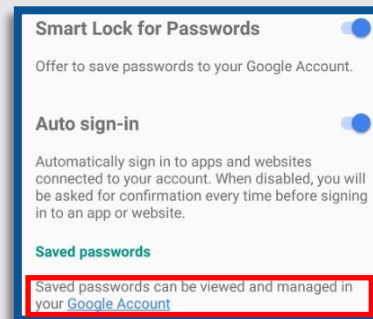
Ads can track everything you do. Not all Android devices and OS versions have settings to turn Ad tracking off. If your device does not have this setting, you can download ad blocking / privacy-oriented browsers or browser add-ons. Here are just a few examples:



Smart Lock for Passwords

From the same Google Settings section, select “Smart Lock for Passwords”. You will then see the screen where you can turn off the options to save your passwords and automatically sign-in to web pages and other account-oriented sites. You can also add apps for which you don’t want passwords to be saved.

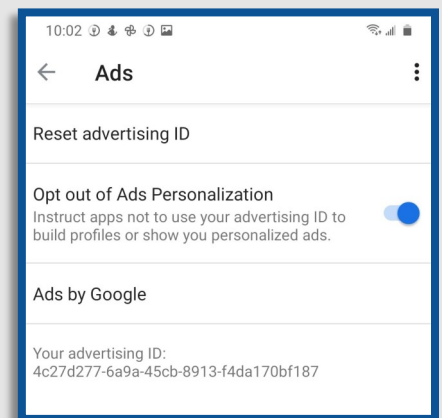
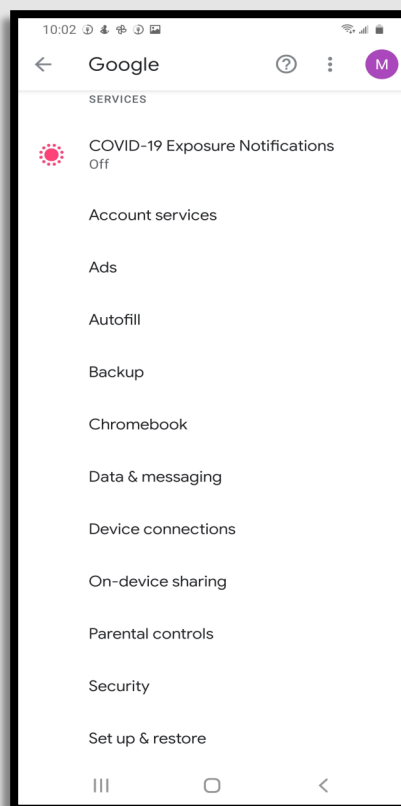
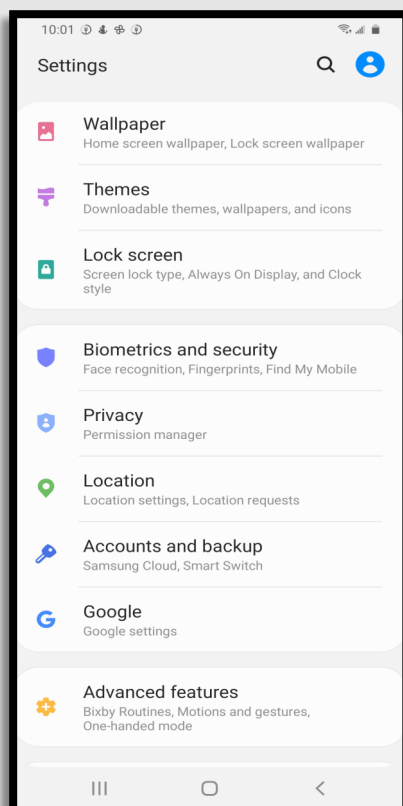
Alternately, you can select specific accounts and delete the saved password by tapping the “Google Account” hyperlink. All saved passwords are encrypted and stored in the Google



cloud storage that comes with your account. Although it is recommended that you turn off the above options, only you can balance your security with the convenience of saved passwords.

If your device has the option to control advertisements, the following directions show you how to disable the feature:

Go to “Settings” > “Google” > “Ads”. Tap the toggle switch to the “On” position for “Opt out of Ads Personalization”.



Safe Browsing: Android devices have a “safe browsing” mode that is built into them and enabled by default. While using Google Chrome, this feature will give warnings before entering a suspicious site. As long as your Chrome and Android are updated to the most recent versions, this feature should work to protect you from malicious sites.

ANDROID PRIVACY SETTINGS (ANDROID 10.0)



Internet Privacy Settings

Browser history and cookies are tracked when browsing the web from your mobile devices. To ensure privacy, open your browser (Chrome) and tap the three dots in the upper right-hand corner. Tap "History" then "Clear Browsing Data" at the bottom (or top) of the screen. On the next screen, select the applicable boxes (use the below screen shot as an example) and tap the blue "Clear Data" button.

You have the option here to tap the drop-down arrow and select a date range of data to be deleted. If you get in the habit of clearing your browser history, cookies, and cache then taking this step will become less important.

Application Manager

The applications you load access different capabilities on your device, regardless of whether they are active or working in the background. You can see, and to some degree control, what access each application has in the "Application Manager".

Go to "Settings" > "Apps" and tap the app you want to view.

Then tap "Permissions".

This will show you what permissions are granted when you accept the user agreement to download the app. In most instances these permissions can be controlled individually.

This only works with apps designed for use specifically with Android. Permissions for older apps or those without full Android functionality can still be disabled, but this could make the app function unreliably.